HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 69–85.
DOI: 10.32567/hm.2025.4.5

Pozderka Gábor[1]

A kibervédelmi és a kiberműveleti gyakorlatok rendszerének átalakulása, az aktuális kihívások vizsgálata

The Transformation of Cybersecurity and Cyber Operations Exercises and the Examination of Current Challenges

Absztrakt

A kibertér az elmúlt évtizedben a biztonságpolitika és a katonai műveletek egyik meghatározó dimenziójává vált. A kibervédelmi és kiberműveleti képességek fejlesztése ennek megfelelően stratégiai jelentőségű feladat mind nemzeti, mind nemzetközi szinten. A felkészülés egyik legfontosabb eszközét a kibervédelmi és kiberműveleti gyakorlatok jelentik, amelyek célja a technikai, szervezeti és vezetői képességek fejlesztése valósághű környezetben. A tanulmány bemutatja e gyakorlatok rendszerének átalakulását, elemzi a fejlődést kiváltó tényezőket, valamint vizsgálja azokat az aktuális kihívásokat – különösen a technológiai fejlődés és a nemzetközi együttműködés területén –, amelyek meghatározzák a gyakorlatok hatékonyságát. Az elemzés rámutat arra, hogy a jövőben a komplex, adaptív és multidiszciplináris megközelítés válik meghatározóvá a kibervédelmi felkészítésben.

Kulcsszavak: kibervédelem, kiberműveletek, kibergyakorlatok, NATO, átalakulás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

Abstract

Cyberspace has become one of the most significant operational domains in modern security and military strategy over the past decade. Consequently, the development of cyber defence and cyber operations capabilities has gained strategic importance at both national and international levels. Cyber defence and cyber operations exercises play a crucial role in preparedness, as they aim to enhance technical, organisational and leadership capabilities in realistic scenarios. This paper examines the transformation of the cyber defence and cyber operations exercise system, analyses the driving factors behind this evolution, and explores current challenges such as rapid technological development and international cooperation. The study highlights that future cyber exercises will increasingly rely on complex, adaptive and multidisciplinary approaches to ensure effective cyber resilience.

Keywords: cyber defence, cyber operations, cyber exercises, NATO, transformation

Bevezetés

A digitalizáció az elmúlt évtizedekben alapvetően átalakította a modern társadalmak működését.[2] Az államigazgatás, a gazdaság, a közlekedés, az energiaszektor, valamint a fegyveres erők működése egyaránt nagymértékben függ az információs és kommunikációs technológiáktól.[3] Az információs rendszerek nem pusztán támogató szerepet töltenek be, hanem sok esetben a működés kritikus feltételét jelentik. Ennek következtében a digitális infrastruktúrák sérülékenysége közvetlen biztonsági kockázattá vált.

A kibertér különlegessége abban rejlik, hogy nem köthető egyetlen ország vagy földrajzi terület határaihoz sem. Emiatt a kibertérben zajló műveletek gyakran rejtve maradnak, az elkövetők kiléte nehezen állapítható meg, miközben a hatásuk szinte azonnal jelentkezik. Egy sikeres kibertámadás nemcsak technikai problémát okozhat, hanem komoly következményekkel járhat az állami működésre, a gazdaságra vagy akár a politikai stabilitásra is. Az ilyen tapasztalatok miatt a kibertér mára a nemzetközi biztonságpolitika egyik meghatározó területévé vált. A kibertér azért is vonzó állami és nem állami szereplők számára, mert viszonylag kevés erőforrással is jelentős hatást lehet elérni benne. Ez különösen azoknak kedvez, akik hagyományos katonai vagy gazdasági értelemben gyengébbek, mégis képesek nyomást gyakorolni fejlett államokra vagy nagy szervezetekre, ennek következtében az erőviszonyok kiegyenlítődhetnek, a konfliktusok jellege is megváltozik, hiszen nem mindig a hagyományos erőfölény lesz a döntő.

A katonai gondolkodásban hagyományosan a szárazföldi, légi, tengeri és később az űrbeli műveletek alkották a hadviselés alapvető doménjeit. A 21. század elejére

[2] A digitális technológiák elterjedése mélyreható változásokat hozott a társadalmak működésében, új módokat teremtett a kommunikációra, a munkavégzésre és az információkezelésre, amelyek alapvetően formálták át a mindennapi életet és az alkalmazott eljárásrendeket.

[3] Kovács 2023.

azonban egyértelművé vált, hogy a kibertér önálló műveleti térként értelmezendő.[4] E felismerést intézményes szinten is megerősítette számos nemzetközi szervezet, különösen a NATO, amely a kiberteret hivatalosan is hadműveleti doménként ismerte el.

A gyakorlatok és felkészülések kiemelt szerepet töltenek be a katonai kiképzések során, mert lehetővé teszik az elméleti ismeretek gyakorlati alkalmazását valósághű körülmények között. Segítenek az érintett állománynak begyakorolni az együttműködést, a fegyelmet és a gyors döntéshozatalt stresszhelyzetekben. A rendszeres felkészülés növeli az egyéni és a csapatszintű teljesítményt, valamint csökkenti a hibák és a félreértések esélyét, illetve a gyakorlatok során feltárhatók a felszerelés, az eljárások vagy a szervezés hiányosságai, amelyeket így időben lehet javítani.

Jelen tanulmány célja a kibervédelmi és kiberműveleti gyakorlatok rendszerének átfogó vizsgálata, különös tekintettel azok átalakulására és az aktuális kihívásokra, ebben a formában kapcsolódik a gyakorlatok hatékonyságértékelési területéhez. A tanulmány bemutatja a gyakorlatok fejlődési ívét, elemzi a technológiai és szervezeti változások hatását, nemzetközi példákon keresztül szemlélteti a különböző megközelítéseket, továbbá ajánlásokat fogalmaz meg a jövőbeni gyakorlatok tervezéséhez. A gyakorlatnak minden esetben összhangban kell lennie a képességfejlesztési célokkal, támogatnia kell azok teljes megvalósulását a DIME[5] minden spektrumában, így direkt módon kapcsolódik a stratégiai döntéshozatali folyamatokhoz és azok kutatási területeihez.

Az összehasonlító elemzés módszertanának alkalmazása a kutatás során biztosítja, hogy a rendelkezésre álló hazai és nemzetközi példákból adekvát következtetéseket lehessen levonni a célok megfogalmazásához, amelyek megfelelő támpontot jelentenek a jövőbeni szervezetek struktúrájának és feladatrendszerének kialakításához.

A kibervédelem és kiberműveletek felértékelődése

A kibertér biztonsági jelentőségének növekedésével párhuzamosan, kezdetben a kibervédelem majd a kiberműveletek szerepe is fokozatosan felértékelődött. A kibervédelem célja nem csupán az informatikai rendszerek védelme, hanem a társadalmi és gazdasági működés folyamatosságának biztosítása is. A kiberműveletek ezzel szemben lehetőséget teremtenek aktív beavatkozásra, elrettentésre és befolyásolásra.[6] Nemzetközi szinten egyre több állam hoz létre dedikált kiberparancsnokságot és fejleszt önálló kiberműveleti doktrínákat. Az Egyesült Államok például az USA Kiberparancsnokság (U.S. Cyber Command) megerősítésével integrálta a kiberműveleteket a hagyományos katonai tervezésbe. Hasonló folyamat figyelhető meg Európában, ahol a legtöbb állam – köztük Észtország, Franciaország, az Egyesült Királyság és Magyarország is – már önálló kibervédelmi és kiberműveleti struktúrákat alakított ki, és folyamatosan vizsgálják azok továbbfejlesztési lehetőségeit.

[4] Clarke–Knake 2019.

[5] A DIME-modell olyan keretrendszer, amely a külpolitikai és stratégiai eszközök négy fő dimenzióját foglalja össze (D – *diplomacy,* I – *information,* M – *military,* E – *economy*), és azt mutatja meg, hogy egy ország vagy szervezet a céljai eléréséhez nemcsak katonai erőt, hanem diplomáciai, információs és gazdasági eszközöket is alkalmazhat, és ezek kombinációja adja a teljes stratégiai hatást.

[6] Haig 2023.

A képességfejlesztés legfontosabb eszközeit a kibervédelmi és kiberműveleti gyakorlatok jelentik. Ezek a gyakorlatok lehetőséget biztosítanak arra, hogy a résztvevők valósághű környezetben teszteljék technikai, szervezeti és vezetési képességeiket, mivel a valós kibertérben ezt csak korlátozottan tehetik meg. A gyakorlatok során nemcsak a technológiai hiányosságok kerülnek felszínre, hanem a döntéshozatali folyamatok, az együttműködés és a kommunikáció gyenge pontjai is. A nemzetközi gyakorlatok különösen fontos szerepet töltenek be, mivel a kibertámadások jellemzően több országot érintenek egyszerre. Az olyan nagyszabású gyakorlatok, mint a NATO által szervezett Cyber Coalition[7] vagy az észt vezetésű, de NATO-képességcélokhoz kapcsolódó Locked Shields,[8] lehetőséget teremtenek az interoperabilitás fejlesztésére és a közös eljárások tesztelésére.

A kibervédelem és kiberműveletek elméleti és fogalmi keretei

A kibervédelem az informatikai rendszerek védelménél jóval komplexebb folyamat. Magában foglalja a technológiai, szervezeti, jogi és humán tényezőket, valamint a stratégiai tervezést. A technológiai komponensek – például tűzfalak, behatolásészlelő rendszerek, titkosítási eljárások – csak a teljes védelem egy részét képezik. A hatékony kibervédelem érdekében szükséges a szervezeti szabályozás, a kockázatkezelés, a tudatosság növelése, valamint a folyamatos oktatás és képzés. A humán tényező kiemelkedő szerepet kap, mivel a felhasználók hibái és a szándékos megtévesztések sokszor nagyobb veszélyt jelentenek, mint a technikai sérülékenységek. Ezért a modern kibervédelemben hangsúlyos a biztonságtudatosság fejlesztése, az incidenskezelési protokollok begyakorlása, valamint a szervezeti kultúra kialakítása, amely elősegíti a gyors és hatékony reagálást.

A kiberműveletek olyan célzott tevékenységek, amelyek a kibertérben fejtenek ki hatást. Ezek lehetnek:

- *védekező műveletek,* amelyek a hálózatok és rendszerek sérülékenységeinek feltárását, a támadások megakadályozását és az incidensek elhárítását célozzák;
- *támadó műveletek,* amelyek a kibertérben a potenciális ellenfél infrastruktúrájára gyakorolnak hatást;[9]
- *befolyásoló műveletek,*[10] amelyek célja a közvélemény, a politikai döntéshozók vagy a szervezeti működés manipulálása.[11]

Fontos megérteni azt, hogy a hagyományos CIS *(communication and information systems)* feladatok főként a katonai kommunikáció és információs rendszerek működtetésére, karbantartására és biztosítására összpontosítanak. Ide tartozik például

[7] A Cyber Coalition a NATO egyik legfontosabb, évente megrendezett kibervédelmi gyakorlata, amelyen a szövetséges és partnerországok vesznek részt. Célja a kibertámadások elleni védekezés, az együttműködés és a döntéshozatali folyamatok gyakorlása valósághű, szimulált környezetben.

[8] A Locked Shields a NATO CCDCOE által szervezett, a világ egyik legnagyobb és legösszetettebb kibervédelmi gyakorlata, ahol a résztvevők valósághű kibertámadások ellen védenek komplex informatikai rendszereket.

[9] Kovács 2021.

[10] AJP 3.20 2020.

[11] Rid 2020.

a rádió- és adatátviteli hálózatok kiépítése, az informatikai rendszerek fenntartása és a megbízható kommunikáció garantálása. Ezzel szemben a kiberszakterület feladatai már nemcsak a rendszerek működtetésére, hanem azok védelmére és az esetleges kibertámadások elleni reagálásra is irányulnak. A kibertevékenységek célja lehet a támadás, a védelem, valamint a sebezhetőségek feltárása és kihasználása. Míg a hagyományos CIS-feladatok statikusabb, inkább működtetési jellegű feladatokat jelentenek, a kiber feladatai dinamikusak és gyorsan változó fenyegetésekkel szembesítenek. A két terület ugyanakkor szoros kapcsolatban áll: a CIS-rendszerek alapozzák meg a kibertevékenységek működését, és azok biztonsága közvetlenül befolyásolja a kiberműveletek sikerét. Összességében a CIS biztosítja a stabil technikai hátteret, míg a kiberszakterület a rendszerek védelmét és az aktív kiberműveletek végrehajtását célozza.

A kiberműveletek során a célok elérése gyakran aszimmetrikus módon történik: kisebb erőforrással rendelkező szereplő is képes jelentős hatást gyakorolni egy fejlettebb rendszerre. Ezért a kiberműveletek alkalmazásának nemcsak technikai, hanem politikai és stratégiai dimenziója is van a korábban hivatkozott DIME minden spektrumában.

Kibervédelmi gyakorlatok: nemzetközi példák

A NATO 2016-os varsói csúcstalálkozóján hivatalosan is elismerte a kibertér mint önálló műveleti domén szerepét.[12] A szövetség tagállamai kötelezettséget vállaltak a kibervédelmi képességek fejlesztésére, valamint az információmegosztás és együttműködés erősítésére.[13] A NATO több nagy léptékű gyakorlatot szervez, például a korábban említett Cyber Coalitiont, amelyben több mint 30 ország vesz részt a védelmi és támadó képességek integrált tesztelésének érdekében. Ezzel összhangban született a NATO felügyelete alatt a Cyber Defence Pledge, amelyben a szövetséges országok elkötelezik magukat a kibervédelmi képességeik fejlesztése és megerősítése mellett. A cél, hogy minden tagállam megfelelő erőforrásokkal és szakértelemmel rendelkezzen a kibertámadások elleni védekezéshez. A kezdeményezés jelentősége abban rejlik, hogy növeli a kollektív védelem hatékonyságát és csökkenti a kibertérből fakadó sebezhetőségeket, emellett elősegíti az együttműködést, a tapasztalatok megosztását és a közös gyakorlatokat a szövetségesek között. Összességében a Cyber Defence Pledge hozzájárul a NATO tagállamai biztonságának és a globális kibertér stabilitásának erősítéséhez.

Az Egyesült Államok 2009-ben hozta létre a U.S. Cyber Commandot, amelynek feladata a nemzeti kiberbiztonsági műveletek koordinálása. A parancsnokság rendszeresen szervez gyakorlatokat, például Cyber Flag néven, ahol a katonai és kormányzati szervezetek komplex kibertámadásokra reagálnak. Ezek a gyakorlatok elősegítik az interoperabilitást a különböző katonai ágak és civil szervezetek között, valamint lehetőséget adnak a döntéshozatali folyamatok tesztelésére.[14]

[12] NATO 2016.
[13] NATO Cyber Defence Pledge.
[14] Libicki 2016.

Észtország 2007-es, ismert kibertámadás-sorozatát követően a szponzor- és partnernemzetek (köztük Magyarország) létrehozták a Locked Shields gyakorlatot, amely a világ egyik legnagyobb valós idejű kibervédelmi gyakorlatává nőtte ki magát. A gyakorlat során a különböző nemzetekből kiválasztott résztvevők valós időben reagálnak szimulált kibertámadásokra, beleértve kritikus infrastruktúrákat, kormányzati hálózatokat és kommunikációs rendszereket. A Locked Shields a stratégiai, taktikai és technikai képességek együttes tesztelését célozza, miközben hangsúlyos a nemzetközi együttműködés.

Izraelben a kibervédelmi gyakorlatok integrált részei a nemzeti biztonsági stratégiának. Az izraeli gyakorlatok során a katonai és polgári szervezetek közösen vesznek részt szimulált támadásokban, amelyek célja a kritikus infrastruktúrák védelme és a gyors reagálás képességének fejlesztése. A gyakorlatok különösen hangsúlyozzák az AI és a prediktív analitika alkalmazását a támadások előrejelzésére.[15]

Japán és Dél-Korea is rendszeresen szervez nagy léptékű kibervédelmi gyakorlatokat, amelyek során a résztvevők valós idejű támadásokra reagálnak. A gyakorlatok során külön figyelmet kap a kritikus infrastruktúrák, például az energia- és közlekedési rendszerek védelme, valamint a kormányzati és katonai kommunikáció folyamatos biztosítása.

Magyarország mind nemzeti, mind kormányzati, mind ágazati szinten több rendszeresen ismétlődő gyakorlat megszervezését is végrehajtotta az elmúlt években, a tapasztalatfeldolgozás eredményeként beépültek a korábbi évek tapasztalatai. A Magyar Honvédség Digitális Csapás nevű többnemzeti kibergyakorlata az állomány technikai felkészültsége mellett a döntéshozatali folyamatok hatékonyságát is rendszeresen teszteli.

A gyakorlatok jellege szerint alapvetően a következő típusokat különböztethetjük meg:

- *Table-top gyakorlatok (TTX).* Szerepjáték-alapú, döntéshozatali folyamatokat vizsgáló gyakorlatok, ahol a résztvevők elméleti forgatókönyvekre reagálnak.[16] Az ilyen jellegű gyakorlatok közelebb hozzák a különböző területeken dolgozó szakembereket, és a kiberbiztonság technikai vetületei mellett annak gazdasági, diplomáciai, politikai, nemzetbiztonsági, vagy akár katonai hatásaira is felhívják a figyelmet. Fontos a valós kibertérben korábban bekövetkezett események ismételt szimulálása, azok továbbgondolása eseményláncok formájában.
- *Red team/blue team gyakorlatok.* A támadó (red) és védő (blue) szerepek elkülönítésével valósághű támadási és védekezési képességeket tesztelnek.
- *Live-fire gyakorlatok.* Valós rendszereken, kontrollált környezetben zajló gyakorlatok, amelyek során a támadások és védekezési mechanizmusok teljes spektruma tesztelhető.
- *Többnemzeti gyakorlatok.* Interoperabilitás és koordináció fejlesztésére irányuló gyakorlatok, ahol különböző országok szervezetei dolgoznak együtt.

[15] Kertész 2023.
[16] Szabó 2018.

A gyakorlatok célja több szinten értelmezhető:

- *technikai szint:* sérülékenységek feltárása, rendszerek megerősítése, incidenskezelési képességek fejlesztése;
- *szervezeti szint:* felelősségi körök tisztázása, kommunikációs folyamatok és koordináció tesztelése;
- *stratégiai szint:* döntéshozatali folyamatok, elrettentési stratégiák és nemzetközi együttműködés erősítése.

Nemzetközi tapasztalatok alapján a rendszeresen végrehajtott gyakorlatok jelentősen növelik a szervezetek felkészültségét, javítják az információmegosztást, és elősegítik a gyors reagálást komplex kibertámadások esetén. Megállapítható, hogy a modern gyakorlatok multidiszciplináris jellegűek, integrálják a technikai, szervezeti és stratégiai szempontokat, valamint hangsúlyozzák a nemzetközi együttműködés jelentőségét. A különböző országok példái azt mutatják, hogy a kibervédelmi gyakorlatok hatékony eszközei a felkészültség növelésének és a kibertérben történő koordinált reagálásnak.[17] A szervezetek saját belső gyakorlatok szervezésével képesek feltárni saját gyengeségeiket, a tapasztalatok alapján javító intézkedéseket bevezetni.

A kibervédelmi gyakorlatok történeti fejlődése és korai szakasza

A kibervédelmi gyakorlatok első generációját elsősorban a technikai problémák megoldására irányuló képzések jellemezték. Az 1990-es évek végén és a 2000-es évek elején a gyakorlatok alapvetően az informatikai szakemberek képzésére koncentráltak, különösen a hálózati biztonság, a tűzfalak konfigurálása, a behatolásészlelés és a sérülékenységek feltárása területén. A gyakorlatok jellemzően izolált környezetben zajlottak, ahol a résztvevők egy előre meghatározott támadási forgatókönyv szerint dolgoztak. Az ilyen gyakorlatok célja elsősorban a technikai hibák és a rendszer-sérülékenységek felismerése volt, ebben a korszakban a szervezeti és vezetési aspektusok kevésbé kaptak hangsúlyt.

Az Egyesült Államokban az 1990-es évek végén és a 2000-es évek elején több kisebb technikai fókuszú gyakorlat zajlott, amelyek célja a katonai hálózatok és a kritikus infrastruktúrák védelmének tesztelése volt. A NATO 2002–2005 között már szervezett kisebb gyakorlatokat, amelyek célja a tagállamok hálózati védelmi képességeinek felmérése és összehangolása volt. Ezek a gyakorlatok fontos alapot teremtettek a későbbi komplexebb rendszerek kialakításához, azonban már a korai tapasztalatok is rámutattak a technikai fókusz korlátaira: az incidensek kezelése gyakran nem volt elég gyors és koordinált, és a szervezeti kommunikáció hiányosságai súlyos problémákat okoztak. Ezen gyakorlatok még jellemzően szeparáltan zajlottak, egy-egy feladat megoldására fókuszáltak, nem vontak be a tervezésbe és feladat-végrehajtásba más műveleti területeket.

[17] Vykopal et al. 2017.

A 2000-es évek közepére egyre világosabbá vált, hogy a kizárólag technikai fókuszú gyakorlatok nem képesek lefedni a kibertér összetett kihívásait.[18] E felismerés nyomán a gyakorlatok komplexebbé váltak, integrálva a szervezeti, vezetői és döntéshozatali dimenziókat. Az újabb gyakorlatok egyik legfontosabb eleme a red team – blue team koncepció bevezetése volt. A red team a támadói szerepet, a blue team a védelmi szerepet testesítette meg. A red team – blue team modellek korai alkalmazása az Egyesült Államokban és az Egyesült Királyságban kezdődött, majd gyorsan átvették más NATO-tagállamok és a szövetség partnerei, ahol a gyakorlatban különböző országok blue teamjei közösen védték a szimulált rendszereket, miközben a red team a támadási technikák széles spektrumát alkalmazta. Kezdetben a nemzetek a red team képességek kialakítását megpróbálták elrejteni többek között a nem egyértelmű, hiányos jogi szabályzói környezet miatt, azonban nyilvánvalóvá vált, hogy ez a narratíva hosszabb távon nem fenntartható, ellehetetleníti a közös feladat-végrehajtást.

A fenti szétválasztás többek között lehetővé tette:

- a támadási módszerek valósághű megértését;
- a védekezési stratégia folyamatos fejlesztését;
- a szervezeti reakciók és döntéshozatali folyamatok tesztelését.

A kibervédelmi gyakorlatok történeti fejlődésében meghatározó jelentőségű volt a kritikus infrastruktúrák bevonása. A 2000-es évek közepén és végén számos országban a gyakorlatok már nemcsak katonai rendszerekre, hanem az energia-, víz-, közlekedési és kommunikációs infrastruktúrákra is kiterjedtek. A korai gyakorlatok egyik fontos hozadéka az volt, hogy lehetőséget adtak az oktatás és tudatosság növelésére. Az oktatási célok mellett a gyakorlatok hozzájárultak a nemzetközi szabványok és protokollok kialakításához, például a NATO és az ENSZ ajánlásainak implementálásához. A gyakorlatok keretében a résztvevők megtanulták felismerni a támadási mintákat, kezelni az incidenseket, koordinálni a szervezeti egységeket és hatékonyan kommunikálni mind belső, mind külső partnerek felé.

A gyakorlatok fejlődésében kulcsszerepet játszott a technológiai fejlődés, amelynek keretében a virtualizáció és szimuláció lehetővé tette a nagy léptékű, valósághű gyakorlatok lebonyolítását anélkül, hogy a tényleges rendszerek veszélybe kerültek volna. Az automatizált támadási szimulációk részeként a mesterséges intelligencia alkalmazása a red team szimulációkban növelte a gyakorlatok komplexitását, valamint a gyakorlatok során keletkező adatok adatgyűjtése és elemzése lehetővé tette a hibák feltárását és a szervezeti tanulás támogatását.

Izrael már a 2000-es évek végén megkezdte a mesterséges intelligencia (AI) integrációját a kibervédelmi gyakorlatokba, különösen a kritikus infrastruktúrák védelmében; ez már előrevetítette egy új korszak érkezését. Az AI-alapú támadásdetektálás és prediktív analitika lehetővé tette a gyors reagálást és a stratégiai döntéshozatal támogatását. A gyakorlatok esetében megfigyelhető, hogy a megkezdett modellek sikere esetén azok igen gyorsan beépülnek a hasonló tematikájú gyakorlatokba. Ennek egyik alapvető oka, hogy a végrehajtó állomány számos esetben átfedéseket mutat,

[18] Bányász–Orbók 2013.

hiszen mind nemzeti, mind nemzetközi téren az anyagi és személyi erőforrások korlátozottan állnak rendelkezésre.

A katonai és állami kibergyakorlatok modern szakasza

A 2010-es évektől a kibergyakorlatok jelentős átalakuláson mentek keresztül.[19] A korai, elsősorban technikai és oktatási célú gyakorlatokat felváltották a komplex, többdimenziós, valós idejű eseményekre reflektáló programok. Az új generációs gyakorlatok célja nem csupán a technikai és szervezeti képességek fejlesztése, hanem a stratégiai döntéshozatal, nemzetközi koordináció és válságkezelés képességének erősítése is. A modern gyakorlatok jellemzője a valós idejű, szimulált támadások komplex integrációja, beleértve a kritikus infrastruktúrákat, a kommunikációs rendszereket, a gazdasági hálózatokat, valamint a kormányzati és katonai irányítási láncokat. A gyakorlatok során a résztvevők különböző szinteken – technikai, operatív és stratégiai – reagálnak az incidensekre, miközben együttműködést gyakorolnak a nemzetközi partnerekkel.

A NATO a 2010-es évekre a kibervédelmi gyakorlatokat már stratégiai eszközként kezelte. A Cyber Coalition gyakorlatok célja a tagállamok közötti interoperabilitás erősítése, a védelmi képességek tesztelése, valamint a döntéshozatali folyamatok gyakorlása volt. A gyakorlatokon a résztvevők valós idejű támadásokra reagáltak, a red team által alkalmazott különböző támadási taktikákra és stratégiákra válaszolva. A Cyber Coalition 2016 már több mint 30 ország részvételével zajlott, fókuszában a kritikus infrastruktúrák védelme és a válságkezelési protokollok tesztelése szerepelt, a Cyber Coalition 2019 gyakorlaton újdonságként a mesterséges intelligencia és automatizált támadási szimulációkat vezették be, a gyakorlat során a résztvevők valós időben reagáltak a komplex kibertámadásokra. A NATO-gyakorlatok jelentősége abban áll, hogy a résztvevők nemcsak technikai készségeiket, hanem stratégiai és koordinációs képességeiket is fejlesztik, ami kulcsfontosságú a többszintű válságkezelésben.

Az Egyesült Államok modern kibergyakorlatainak továbbra is központi eleme a U.S. Cyber Command által szervezett Cyber Flag sorozat. A gyakorlatok célja folyamatos átalakuláson ment keresztül; a katonai és civil kiberműveletek integrációja, a támadó és védelmi képességek tesztelése, valamint a döntéshozatali folyamatok felgyorsítása fontos célok. A gyakorlatok egyik kiemelkedő aspektusa a többszintű koordináció: a helyi katonai parancsnokságok, szövetségi ügynökségek és külső partnerek együttműködésének tesztelése.

Észtország a modern kibervédelmi gyakorlatok esetében is az élvonalban áll, többek között a Locked Shields gyakorlat tapasztalatai révén. A résztvevők valós idejű támadásokra reagálnak, amelyek célja a kritikus infrastruktúrák, a kormányzati hálózatok és a kommunikációs rendszerek védelme. A Locked Shields gyakorlat különlegessége a széles körű nemzetközi részvétel, a gyakorlat során a résztvevőknek interoperábilis módon kell együttműködniük. A gyakorlat során hangsúlyos a red team

[19] Şeker 2019.

által alkalmazott aszimmetrikus támadások kezelése, valamint a gyors döntéshozatal és válságkezelés képessége.[20]

Izrael hosszú ideje kiemelt figyelmet fordít a kibervédelmi képességek fejlesztésére, különösen a kritikus infrastruktúrák védelmére és a stratégiai döntéshozatal támogatására. Az izraeli gyakorlatok során integrálják a katonai és polgári szervezeteket, a red team támadások és blue team védekezések valós idejű koordinációját, valamint a mesterséges intelligencia és prediktív analitika alkalmazását.

Összhangban a korábban megfogalmazottakkal, a 2010-es évektől kezdve több fontos trend figyelhető meg:

- *valós idejű szimulációk:* a gyakorlatok komplexitása nőtt, a résztvevők valós időben reagálnak a támadásokra;
- *AI és prediktív analitika:* a mesterséges intelligencia alkalmazása a támadásdetektálásban és a válságkezelés támogatásában;
- *kritikus infrastruktúrák integrálása:* az energia-, víz-, közlekedési és kommunikációs rendszerek védelme prioritás;
- *többnemzeti együttműködés erősítése:* a gyakorlatok során a résztvevők interoperábilis módon dolgoznak együtt, növelve a nemzetközi felkészültséget;
- *aszimmetrikus támadások kezelése:* a red team komplex és kreatív támadásokat alkalmaz, amelyek aszimmetrikus kihívásokat jelentenek a blue team számára.

A modern katonai és állami kibergyakorlatok komplex, multidimenzionális rendszerek, amelyek integrálják a technikai, szervezeti és stratégiai aspektusokat. A modern gyakorlatok elősegítik a kibervédelmi képességek folyamatos fejlesztését, támogatják a kritikus infrastruktúrák védelmét, és lehetőséget biztosítanak az új technológiák, például az AI integrációjára a kiberműveletekben.

Magyarország mint a NATO tagja aktívan részt vesz a korábban felsorolt nemzetközi kibergyakorlatokban, így biztosítva a szövetséges rendszerből adódó képességfejlesztési célok megvalósulásának tesztelését, finomhangolását.[21]

A kibervédelmi és kiberműveleti gyakorlatok aktuális kihívásai

A 21. század második évtizedében a kibervédelmi és kiberműveleti gyakorlatok nem csupán technikai képzések, hanem komplex stratégiai eszközök is. Az esettanulmányok elemzése lehetővé teszi, hogy a gyakorlatok különböző típusait, célkitűzéseit és eredményeit konkrét példákon keresztül vizsgáljuk. A hivatkozott nemzeti és nemzetközi gyakorlatok jelentősek katonai, állami és kritikus infrastruktúrákat érintő felkészültség szempontjából. A korábban felsorolt példák alapján egyértelműen megállapítható, hogy a modern kibergyakorlatok multidimenzionálisak, és nemzetközileg koordináltan kell megvalósulniuk.

A kibervédelmi gyakorlatok folyamatos fejlődésének egyik legfontosabb aspektusa a folyamatosan változó fenyegetési környezethez való alkalmazkodás. Az új

[20] NATO CCDCOE 2022.
[21] Szöllősi 2024.

típusú kibertámadások, a technológiai innovációk, a globális geopolitikai folyamatok és a kritikus infrastruktúrák komplexitása új kihívásokat jelent a gyakorlatok tervezése és lebonyolítása szempontjából. A modern gyakorlatok tervezése során meg kell hogy jelenjenek a kiberbűnözők és az államilag támogatott csoportok által használt eljárásokra adott válaszok, a résztvevőknek képesnek kell lenniük mindkét típusú támadás kezelésére, figyelembe véve a különböző támadási módszerek komplexitását.

A tapasztalatok elemzése alapján az alábbi szempontok figyelembevétele elengedhetetlen a képességfejlesztés során.

A nemzetközi együttműködés fontossága

A kibertér határokon átnyúló jellege miatt a kibertámadások ritkán érintenek csak egyetlen államot, ezért önálló nemzeti válaszok gyakran nem elegendők. A támadások forrásának azonosítása és a hatások kezelése sokszor több ország információinak és képességeinek összehangolását igényli. A nemzetközi együttműködés a kibergyakorlatok során lehetővé teszi a közös eljárások, kommunikációs csatornák és döntéshozatali mechanizmusok tesztelését. Ennek hiányában válsághelyzetben lassú vagy ellentmondásos reakciók alakulhatnak ki. A közös gyakorlatok során a résztvevők megismerik egymás képességeit és korlátait, ami növeli a bizalmat és a hatékony együttműködés esélyét valós helyzetekben. Az eltérő tapasztalatok és megközelítések megosztása hozzájárul a jobb védekezési módszerek kialakításához is. Mindez összességében erősíti a kollektív kibervédelmet, és csökkenti a kibereseményekeszkalálódásának kockázatát.

A technológiai innovációk integrálása

A kibertérben megjelenő fenyegetések folyamatosan fejlődnek, ezért a védekezési módszereknek is lépést kell tartaniuk ezekkel a változásokkal. Ha a kibergyakorlatok nem építik be az új technológiai innovációkat, akkor nem tükrözik a valós környezetet, és hamis biztonságérzetet kelthetnek. Az új eszközök és megoldások integrálása lehetővé teszi a modern támadási technikák és sérülékenységek valósághű szimulációját. Ennek következtében a résztvevők megtanulják kezelni azokat a kihívásokat, amelyekkel tényleges műveleti helyzetben is szembesülhetnek. A technológiai innovációk alkalmazása segít feltárni a meglévő rendszerek gyenge pontjait, még azelőtt, hogy azokat egy valódi támadás kihasználná. Emellett elősegíti az új védelmi megoldások kipróbálását és finomítását ellenőrzött környezetben. Mindez hozzájárul ahhoz, hogy a szervezetek rugalmasabbá és ellenállóbbá váljanak, és hatékonyabban tudjanak reagálni a gyorsan változó kibertér kihívásaira.

A kritikus infrastruktúrák védelme prioritás[22]

A kritikus infrastruktúrák – például az energiaellátás, a közlekedés, a vízellátás vagy a kommunikációs rendszerek – működése alapvetően meghatározza a társadalom mindennapi életét. Ha ezek a rendszerek kibertámadás következtében megbénulnak, annak azonnali és súlyos következményei lehetnek a lakosság biztonságára és a gazdaság működésére nézve. Éppen ezért a kibergyakorlatok során kiemelt figyelmet kell fordítani ezen rendszerek védelmére, illetve arra, hogy a valós kockázatokat tükröző helyzeteket lehessen modellezni. A gyakorlatok lehetőséget adnak arra, hogy feltárják a kritikus infrastruktúrák sebezhetőségeit és a különböző ágazatok közötti függőségeket; ennek hiányában egy valódi támadás során a reakciók lassúak vagy összehangolatlanok lehetnek, ami tovább növeli a károk mértékét. Mindez hozzájárul a rendszerek ellenálló képességének növeléséhez, és csökkenti annak esélyét, hogy egy kibertámadás társadalmi vagy nemzetbiztonsági válsággá alakuljon.

A red team – blue team módszertan hatékonysága

A red team – blue team módszertan alkalmazása azért elengedhetetlen a kibergyakorlatok során, mert valósághű módon modellezi a támadó és a védekező oldal közötti dinamikát. A red team támadóként folyamatosan új technikákat és megközelítéseket alkalmaz, ami arra kényszeríti a blue teamet, hogy éles helyzetekhez hasonló környezetben reagáljon. Ennek hatására a védekező oldal nemcsak az eszközeit, hanem döntéshozatali folyamatait és együttműködését is fejleszti. A módszertan lehetővé teszi a védelmi rendszerek gyenge pontjainak feltárását még azelőtt, hogy azokat egy valódi támadás kihasználná. A folyamatos támadás-védekezés ciklus miatt a résztvevők azonnali visszajelzést kapnak a stratégiáik hatékonyságáról. Összességében a red team – blue team megközelítés növeli a kibergyakorlatok realizmusát, és hozzájárul a szervezetek hosszú távú kibervédelmi felkészültségének erősítéséhez.

A stratégiai és döntéshozatali képességek fejlesztése

A stratégiai és döntéshozatali képességek fejlesztése fontos feladat a kibergyakorlatok során, mert a kibertámadások gyakran komplex és gyorsan változó helyzeteket teremtenek. Ha a döntéshozók nem tudnak gyorsan és helyesen reagálni, a támadás hatásai elhatalmasodhatnak, és súlyos következményekkel járhatnak a kritikus rendszerekre és a társadalomra is. A gyakorlatok lehetőséget adnak arra, hogy a résztvevők valósághű szimulációkban gyakorolják a döntéshozatalt, a prioritások meghatározását és a kockázatok értékelését, ez elősegíti, hogy a valós helyzetekben a vezetők nyugodtabban és átgondoltabban reagáljanak majd. A stratégiai gondolkodás fejlesztése javítja az erőforrások optimális elosztását és az együttműködést a különböző szervezeti egységek között. Mindez csökkenti a hibák kockázatát, növeli a válsághelyzetek

[22] ENISA 2024.

kezelhetőségét, és erősíti a szervezet ellenálló képességét a kibertámadásokkal szemben. Összességében a stratégiai képességek gyakorlása nélkül a technikai készségek önmagukban nem elegendők a hatékony védekezéshez. A gyakorlatok nemcsak technikai, hanem szervezeti és stratégiai szinten is fejlesztik a résztvevőket.

A technikai képességek mellett a szervezeti és stratégiai dimenziók szerepe egyre fontosabb:

- *gyors döntéshozatal:* a valós idejű támadások gyors reagálást igényelnek;
- *koordináció több szervezet között:* a katonai, kormányzati és privát szektorbeli szereplők közötti együttműködés kritikus;
- *kommunikációs kihívások:* a támadások során a belső és külső kommunikáció hatékony kezelése alapvető, a stratégiai kommunikáció szerepe felértékelődik;
- *jogi kihívások:* a jól felkészített technikai állomány mellett a kibertérben végrehajtott műveletek során rendkívül fontosak a jogi és szabályzó környezetet jól ismerő szakemberek. A kibertéri műveletek jogi kereteinek tisztázása kulcsfontosságú;
- *adatvédelmi és adatmegosztási szabályok:* különböző országok eltérő szabályozása nehezíti az interoperabilitást.

A gyakorlatok során várható jövőbeli trendek

A kritikus infrastruktúrák digitalizációja és az IoT-[23] (Internet of Things) alapú rendszerek elterjedése jelentősen növelte a kitettséget és sebezhetőséget. A gyakorlatok abban az esetben lehetnek hatékonyak és sikeresek, amennyiben ezen kihívásokra képesek választ adni, képesek szimulálni a valós környezetet. Ennek megfelelően, a jelenleg végrehajtott gyakorlatok során a résztvevőknek képesnek kell lenniük a hálózatok integrált védelmére, a valós idejű támadásfigyelésre, a rendszerek gyors helyreállítására és a koordinált válságkezelésre.

A jelenlegi tapasztalatok alapján a kibervédelmi gyakorlatok jövőbeni tervezése során az alábbi fontos irányok azonosíthatók és várhatók:

- *integrált szimulációk:* a fizikai és digitális rendszerek együttes védelme;
- *AI és automatizálás fokozása:* az emberi döntéshozatal kiegészítése prediktív analitikával;
- *nemzetközi standardizáció:* protokollok és gyakorlatok összehangolása a globális interoperabilitás érdekében;
- *aszimmetrikus és hibrid fenyegetések kezelése:* állami és nem állami szereplők komplex támadásai;[24]
- *tudatosság és képzés kiterjesztése:* nemcsak a szakemberek, hanem döntéshozók és szervezeti vezetők bevonása.

[23] A dolgok internete (IoT) lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internetalapú hálózaton egy másik eszközzel kommunikálni.

[24] Resperger 2018.

A kibervédelmi és kiberműveleti gyakorlatok tehát dinamikusan alkalmazkodnak a változó fenyegetésekhez, és a nemzetközi együttműködés, valamint a technológiai innováció kulcsfontosságú szerepet játszik a hatékonyság növelésében. A fenyegetési környezet komplexitása és a kritikus infrastruktúrák növekvő sebezhetősége új képességeket igényel a résztvevőktől, a szervezeti, döntéshozatali és nemzetközi koordináció kulcsfontosságú a gyakorlatok sikeréhez. A technológiai innovációk új kihívásokat, de egyben lehetőségeket is kínálnak, a nemzetközi együttműködés és jogi harmonizáció elengedhetetlen a globális kibervédelmi képességek fejlesztéséhez.[25] Ezek a gyakorlatok már nem csupán tréningek, hanem komplex, stratégiai szintű eszközök a nemzetközi biztonsági képességek fejlesztésében. A gyakorlatok hatékonyságának értékelése alapvető annak érdekében, hogy a résztvevők ne csak a szimulációkban, hanem a valós rendszerekben is képesek legyenek megfelelően reagálni. A hatékonyság vizsgálata magában foglalja a technikai, operatív és stratégiai szinteket, a szervezeti tanulságokat, valamint az interoperabilitás és döntéshozatal fejlesztését.

A gyakorlatok hatékonyságának értékelésére több módszer létezik (kvantitatív, kvalitatív, kombinált), amelyeket kombináltan célszerű alkalmazni. Példaként említhető, hogy a NATO Cyber Coalition gyakorlatokban a red team támadások sikeressége mérhető, azonban a blue team és a részt vevő országok koordinációs képessége kvalitatív módon értékelhető. A Locked Shields gyakorlaton minden csapat pontozása a támadások elleni védekezés, a válaszidők és a kritikus rendszerek védelmének sikeressége alapján történik, a gyakorlat után a részt vevő országok konkrét biztonsági protokollokat és eljárásokat módosítanak saját nemzeti rendszereikben.[26]

Általános következtetések és jövőbeli ajánlások

A kibervédelmi gyakorlatok nem csupán technikai tréningek, hanem komplex stratégiai eszközök, amelyek javítják a döntéshozatali és válságkezelési képességeket, fejlesztik a nemzetközi interoperabilitást, tesztelik a kritikus infrastruktúrák és kommunikációs hálózatok védelmi képességeit.

A gyakorlatokban egyre nagyobb szerepet kapnak az alábbi technológiák:

- *mesterséges intelligencia (AI):* támadásdetektálás, prediktív analitika, automatizált reagálás;
- *IoT és 5G-rendszerek:* kritikus infrastruktúrák és kommunikációs hálózatok integrált védelme;
- *felhőalapú rendszerek:* decentralizált támadások kezelése, redundancia és reziliencia biztosítása.

Az alábbi szempontok azonosíthatók mint kritikus kihívások és korlátok:

- *fenntarthatóság:* a gyakorlatok költség- és erőforrásigénye magas, különösen a fejlett technológiák alkalmazása esetén;

[25] Menczelesz 2025.
[26] Ertan et al. 2020.

- *szervezeti ellenállás:* az új protokollok és eljárások implementálása gyakran kulturális és szervezeti akadályokba ütközik;
- *jogszabályi korlátok:* a nemzetközi együttműködés során az adatvédelmi és jogi szabályozások eltérései nehezítik az interoperabilitást;
- *technológiai kompatibilitás:* a gyakorlatokon tesztelt innovációk nem mindig kompatibilisek a meglévő rendszerekkel.

A jövőben a gyakorlatok egyre inkább ötvözni fogják a fizikai és digitális rendszereket, a katonai, kormányzati és civil szektort,[27] valamint a valós és szimulált fenyegetéseket, a mesterségesintelligencia-alapú támadásdetektálás,[28] prediktív analitika és automatizált válaszmechanizmusok kulcsfontosságúak a komplex kibertámadások kezelésében. A kibervédelmi és kiberműveleti gyakorlatok stratégiai, technológiai és szervezeti szinten egyaránt kritikus szerepet töltenek be a nemzetközi biztonság és a kritikus infrastruktúrák védelmében. A gyakorlatok értékelése és a tapasztalatok átültetése a valós rendszerekbe javítja a döntéshozatalt, a koordinációt és a technológiai reagálóképességet. A jövőbeli trendek az integrált szimulációk, az AI-alapú automatizált védelem, az IoT-integráció és a nemzetközi standardizáció felé mutatnak. Az ajánlások megvalósítása elősegíti a kibervédelmi képességek folyamatos fejlesztését, a nemzetközi együttműködés megerősítését és a kritikus infrastruktúrák biztonságának növelését.[29] A tanulmányban feldolgozott példák alapján megfogalmazott ajánlások a gyakorlatok fejlesztésére, amelyeknek összhangban kell lenniük a szervezet képességfejlesztési céljaival:

- *Integrált értékelési keretrendszer kialakítása.* Kombinálni kell a kvantitatív és kvalitatív módszereket, figyelembe véve a technikai, szervezeti és stratégiai dimenziókat.
- *Technológiai innovációk folyamatos integrálása.* AI, automatizált támadásdetektálás, felhő- és IoT-rendszerek folyamatos tesztelése és fejlesztése.
- *Nemzetközi együttműködés erősítése.* Közös protokollok, adatmegosztási standardok és interoperabilitás kialakítása.
- *Képzés és tudatosság növelése.* A gyakorlatokba bevonni vezetőket, döntéshozókat és nem csak technikai személyzetet.
- *Kritikus infrastruktúrák védelmének prioritása.* A fizikai és digitális rendszerek integrált védelmének gyakorlása valós idejű támadásszimulációkkal.
- *Jogi és szabályozási harmonizáció.* Az adatvédelmi és jogi keretek egységesítése a nemzetközi gyakorlatok során, valamint közös válságkezelési forgatókönyvek kidolgozása.[30]

A jövőben a gyakorlatok célja egyre inkább az emberi döntéshozatal kiegészítése és a reakcióidő csökkentése, a valós infrastruktúrák valós idejű tesztelése, valamint a gyors helyreállítási és redundanciastratégiák fejlesztése lesz. A gyakorlatok során megszerzett tapasztalatok alapján szükséges a nemzetközi protokollok, szabványok

[27] Kiss 2019.
[28] Zacharis–Katos–patsakis 2024.
[29] NATO 2025.
[30] Schmitt 2017.

és adatmegosztási eljárások harmonizálása, az interoperabilitás javítása révén a többnemzeti válaszok hatékonyabbá válhatnak. Szükséges továbbá, hogy a gyakorlatok eredményei beépüljenek a kibervédelmi és kiberműveleti stratégiákba, válságkezelési és koordinációs eljárásokba figyelembe véve a fenyegetési trendeket.[31]

A Magyar Honvédség a kiberműveleti gyakorlattervezés és végrehajtás során megkezdte a fenti ajánlások implementálását, az eseményláncokat folyamatosan aktualizálja a megszerzett tapasztalatok alapján. A kibervédelemben érintett szervezetek közösen vizsgálják a DIME spektrumában történő feladat-végrehajtás kihívásaira adható válaszokat, ezzel összhangban aktualizálják a szabályzói keretrendszert. Szinte bizonyos, hogy a közeljövőben új, ma még nem azonosított kihívások fognak megjelenni, amelyekre csak akkor adható gyors és hatékony válasz, ha a jelenleg kialakított folyamatok már készségszintűek.

Felhasznált irodalom

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(E-szám), 188–209. Online: https://ojs.mtak.hu/index.php/hadtudomany/article/view/6705/5304

Clarke, Richard A. – Knake, Robert K. (2019): *The Fifth Domain*. [H. n.]: Penguin Books. Online: www.penguinrandomhouse.com/books/600219/the-fifth-domain-by-richard-a-clarke-and-robert-k-knake/

ENISA (2024): *Cyber Europe 2024: Unveiling Key Insights From the Cyber Exercise That Tested the Cybersecurity of EU's Energy Sector.* Online: www.enisa.europa.eu/news/cyber-europe-2024-unveiling-key-insights-from-the-cyber-exercise-that-tested-the-cybersecurity-of-eus-energy-sector

Ertan, A. et al. szerk. (2020): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn: CCD COE. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Haig Zsolt (2023): A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/102124?key=Kiberv%C3%A9delem%20%C3%A9s%20nemzetbiztons%C3%A1g%20kiss

Kertész Bence (2023): Kiberműveletek az Izrael és Hamász közötti háborúban. *biztonságpolitika.hu,* 2023. október 30. Online: https://biztonsagpolitika.hu/cikksorozatok/kibermuveletek-az-izrael-es-hamasz-kozotti-haboruban

Kiss Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37. Online: https://real.mtak.hu/125219/1/HSZ_2019_147_4_Kiss_Almos_Peter.pdf

[31] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

Kovács László (2021): Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Libicki, Martin (2016): *Cyberspace in Peace and War.* Annapolis, MD: Naval Institute Press. Online: https://books.google.hu/books/about/Cyberspace_in_Peace_and_War.html?id=m4f9DAAAQBAJ&redir_esc=y

Menczelesz Adrián (2025): Digitális védelem a 21. században – hazánk kiberbiztonsági stratégiája és annak megvalósítása. *Jogászvilág,* 2025. június 5. Online: https://jogaszvilag.hu/napi/digitalis-vedelem-a-21-szazadban-hazank-kiberbiztonsagi-strategiaja-es-annak-megvalositasa/#

NATO (2016): *Warsaw Summit Communiqué.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2025): *NATO Cyber Coalition 2025. Advancing Cyber Defence and Strengthening Alliance Resilience.* Online: www.act.nato.int/article/cyber-coalition-2025/

NATO CCDCOE (2022): *NATO Cyberspace Exercises: Moving Ahead CyCon 2022 Workshop Summary.* Online: https://ccdcoe.org/library/publications/nato-cyberspace-exercises-moving-ahead-cycon-2022-workshop-summary/

NATO Cyber Defence Pledge (2016). Online: www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge

NATO Standard Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations (2020). Online: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Resperger István (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus. Online: https://bit.ly/4sFA7Gx

Rid, Thomas (2020): *Active Measures. The Secret History of Disinformation and Political Warfare.* London: Profile Books. Online: https://books.google.hu/books/about/Active_Measures.html?id=lWltDwAAQBAJ&redir_esc=y

Schmitt, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Şeker, Ensar (2019): The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. *arXiv:1906.03184.* Online: https://doi.org/10.1109/CyberSecPODS.2018.8560673

Szabó András (2018): Ajánlás TTX gyakorlatok szervezéséhez. *Hadmérnök,* 13(KÖFOP), 235–251. Online: www.hadmernok.hu/180kofop_14_szabo.pdf

Szöllősi Gergely (2024): Locked Shields 2024: Kimagasló magyar eredmény. *Honvédelem,* 2024. május 21. Online: https://honvedelem.hu/hirek/locked-shields-2024-kimagaslo-magyar-eredmeny.html

Vykopal, Jan et al. (2017): Timely Feedback in Unstructured Cybersecurity Exercises. *arXiv:1712.09424.* Online: https://doi.org/10.48550/arXiv.1712.09424

Zacharis, Alexandros – Katos, Vasilios – Patsakis, Constantinos (2024): Integrating AI-Driven Threat Intelligence and Forecasting in the Cyber Security Exercise Content Generation Lifecycle. *International Journal of Information Security,* 23(4), 2691–2710. Online: https://doi.org/10.1007/s10207-024-00860-w